Quantum Applications in Political Science

Research Thesis

Presented in partial fulfillment of the requirements for graduation *with research distinction* in Political Science in the undergraduate colleges of The Ohio State University

by

Caleb Costa

The Ohio State University

April 2020

Project Advisor: Professor Skyler Cranmer, Department of Political Science

Abstract

This paper will show the current state of quantum computation and its application as a political science research method. It will look at contemporary empirical literature to assess the current state of the method in both political science and computer science. Then, by assessing the state of quantum computation, this paper will make predictions concerning quantum computation as a research tool and also assess its capability as a catalyst for international diplomacy and discourse. Quantum computation is an emerging technology with increasing scientific attention. This paper will use IBM's quantum computer, accessed through the cloud, to model and execute quantum algorithms that show the utility for political science research. Furthermore, through the base mathematics of common quantum algorithms, this paper will show how these algorithms can be expanded. This paper finds that quantum computation is a valuable tool with remarkable potential. However, quantum computing has its limitations and currently resides in an important juncture that will decide whether technology involving it will be resigned as a niche theoretical tool or be continued to be developed into a mainstream technology.

Introduction

The goal of this paper is to bridge the gap between quantum computing and political science by first explaining the technical concepts of quantum computing and then showing its possible uses. The hope is that by learning more about quantum computing technicals, political science researchers will be more able to determine useful quantitative cases and also consider the technology easier in descriptive studies.

Quantum computing is here. It is being used by researchers in fields across academia and private industry. However, the adaptation of quantum computing is lacking in the social sciences and in Political Science research in particular. This could be so for many different reasons. The technology may seem like a daunting tool meant for the sole use of computer scientists and physicists. Quantum computers haven't yet met the requirements to be universal and finding one to use takes considerable effort. In this vein, quantum computers are probably at a similar state that "classical" computers were in the 70's and 80's, useful for some niche tasks but not abundantly useful for any number of general tasks. This paper is meant to dissuade the previous or possible answers for its confined adaptation. By taking a pedagogical approach to quantum computing, this paper will hopefully encourage the political science community to engage with quantum computing as a research tool and as a possible policy problem.

The first few sections might scare you away from using or thinking about quantum computing. However, by struggling and persevering through the first sections you will hopefully realize in the pages that follow that quantum computing is not as terrifying as the quantum mechanics and linear algebra may make it seem. By understanding and tangling with these concepts you will be better able to concretely apply quantum computing to your

research or be better able to demystify the policy consequences. While Quantum Computers are massive feats of human engineering they are also simplified through API's and interfaces. You can therefore leverage your soon to be acquired hardware knowledge to better leverage tools such as IBMQ. In matters of policy, instead of understanding what quantum computers are capable of you will understand why they are capable of doing what they can. You can read surface level articles about the repercussions of quantum computers solving encryption. At the end of this paper you will be able to understand how this happens and further comprehend why quantum computers may be powerful in niche situations while not actually being a dark scary threat to all types of technology. Furthermore, quantum computation presents interesting questions for security studies and global diplomacy. While some literature has been published in this area, there are far more potential areas of research.

Section 1: Quantum Science and Computation

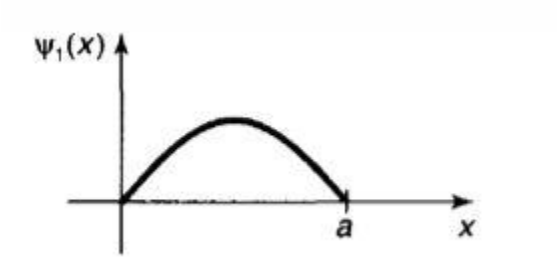
Quantum Mechanics

The following section will give an overview of quantum physics and its underlying mathematics. This is not meant to be a full lesson and is in no way a fully inclusive teaching of quantum mechanics. Instead these are general concepts that will help with the underlying aspects of quantum computing technology. Quantum mechanics will aid in understanding the core differences of classical and quantum computers and better reveal the potential and limitations of quantum computation.

Quantum physics delves into the most minuscule parts of physics, at a level characterized as sub-atomic and works with what is called a **wave function**. This isn't tangible or real but is instead a mathematical construction that is used to predict how electrons act. A wave function is essentially a probability distribution. A macro way of looking at this process is that "Quantum" is the wave function or probability distribution that we construct and what we actually see is an electron. The electron is measured with the Quantum wave function and it is this measurement that collapses the wave function and reveals a true state. This wave function of an electron is mapped using Schrodinger's equation. A full mathematical is not essential but for the mathematically curious the equation is:

$$-\frac{\hbar^2}{2m_e}\left(\frac{\partial^2\Psi}{\partial x^2}+\frac{\partial^2\Psi}{\partial y^2}+\frac{\partial^2\Psi}{\partial z^2}\right)+V(x,y,z)\Psi=i\hbar\frac{\partial\Psi}{\partial t}.$$

The important piece of this equation is the variable psi: Ψ. This is the probability function that maps the wave. The absolute value of the amplitude at any point on x squared is the probability that an electron is at that position. For example, the probability of the electron being at point a in the graph below would be zero. The highest probability would be at the maximum in between a and the axis.



The quantum wave function is the base of quantum physics and quantum computation. A proper understanding of this principle is integral and will further make the following concepts more intuitive.

Superposition is the adding together of waves or the ability for a quantum system to be in multiple states at the same time. This is simply a logical step from the wave function. The wave function is a probability distribution. As such, an electron can have a high likelihood of being in multiple places at once. This duality is what is known as superposition. Schrodinger's Cat is a thought experiment performed around the conception of quantum physics that helps better explain superposition while also exposing the paradoxical nature of the wave function. Schrodinger imagined a cat placed in a sealed box that contained a device that had a 50 percent chance of killing the cat and a 50 percent chance of nothing happening. After an hour, the box would be opened and the cat would be observed. Would the cat be alive or dead? By looking into the box, one should be able to make a definitive observational choice. However, according to quantum physics, right

before opening the box, the cat would be in a superposition where it would be equally 50% dead and 50% alive. It is only upon opening the box that the cat would be observed as a single state. A cat cannot be both alive and dead and it is this paradoxical nature that alludes to one of the great mysteries of quantum physics. The collapse of the wave function from superposition to its observed state is still not fully understood and is known as the measurement barrier. However, the important objective for our use in quantum computation is to understand superposition: the ability for an electron to be in multiple states at once.

Entanglement is the interaction between two or more waves by which the waves become intertwined and connected. Once entangled, the two waves become linked and computationally correlated. By interacting with one wave function you are directly influencing the other wave. This becomes helpful later as quantum entanglement allows for increased computation power.

Quantum Computing History

Quantum computing history can be effectively split into two distinct periods: pre-1994 and post. Before 1994, quantum computing theorists were considered to be on the fringe. There were plenty of discoveries within the field of quantum physics and the subfield of quantum computing leading up to 1994 but none were taken too seriously by mainstream academics or industry. Quantum computing was deemed an interesting but quirky theoretical idea with little applicable use. Bell proved that there was no classical explanation for quantum mechanics in 1964. No Cloning Theorem was established by Wootters and Zurek in 1982 which states that a single unknown quantum state cannot be

duplicated (Wootters and Zurek in 1982). Each of these discoveries were celebrated in the field of physics but their greatest contribution was perhaps the influence of a 1994 paper by Simon. He used periodicity to prove that factoring and discrete logarithm problems could be solved exponentially faster using a quantum computer. Peter Shor then took this one step further by describing his algorithm, Shor's algorithm, which discovered a way for a quantum computer to factory immensely large integers in a short period of time. This algorithm will be discussed in detail later, but Shor's algorithm catalyzed a worldwide interest in the construction of quantum computers. In 1997, the first quantum computer was created but it was very small and not particularly useful other than providing a base. The more modern quantum computers began to appear after 2007 when Canadian startup D-wave created a quantum computer 12 times the size of the original 1997 quantum computer. Current quantum computers max out at 53-54 qubits. For now, qubits can be considered equivalent to computing capacity, the more qubits the better.

While all quantum computers use quantum bits there are different approaches towards computational structure. Currently there are two separate approaches for implementing quantum computation: Analog and Universal. Analog approaches further branch off into different niche categories. Analog quantum computation is usually used for a specific purpose. Quantum simulation with classical supercomputers is an analog approach that has a low ceiling but provides a good intermediate tool. It temporarily solves a later explained problem of decoherence which inhibits the effectiveness of quantum computers. Quantum annealing, a second analog approach, is a specialty type of quantum computing that can only solve optimization problems. Neither of these two approaches have the potential that universal quantum computers do. It is more general and uses

quantum logic gates to solve problems. The rest of this paper will focus almost solely on this type of quantum computer. While analog methods are useful intermediaries and their existence should be known, the future of quantum computing is the universal quantum computer.

Classical vs Quantum Computing

This section will now use previously explained quantum mechanics to show the difference between classical and quantum computing. By understanding the technical differences, one will be able to better determine potential uses for technology.

The most basic unit of information in a normal computer or "classical computer" is the bit. It is a logical state and contains one of two values: 0 or 1. More bits means more stored information and more computing power. Today's classical computers have around 240 gigabytes of storage. The quantum equivalent of the bit is **the qubit** which acts somewhat differently than a classical bit but arrives at a similar final state of 0 or 1. If you have some knowledge of quantum computing you may have read that what makes quantum computing unique is the ability for a qubit to be in many states at once. This isn't perfectly true, but it is a useful macro conception. The reality is that if a qubit is in superposition, it is thus in a range of probabilities up until the qubit is measured. Think of the qubit as the electron in the quantum mechanics section, it has a range of probabilities that collapse into a single state once measured. In fact, most quantum computers use the charges of electrons, photons or ions as the numerical measurement for qubits. In order to measure superpositions you would not only need the numeric outcome, 1 or 0, but a coefficient of all the probabilities. For a two-bit classical computer, you would only need

the single two-bit outcome. For a two-qubit quantum computer you would need the coefficients for the four possible states. In this way two qubits have four bits of actual information stored in them. This means that the equivalent amount of classical information contained by N qubits is 2^n bits. Therefore, 300 qubits in superposition would be equivalent to 2^{300} classical bits of information which is as many particles as there are in the universe. This is the amazing thing about quantum computers. They have incredible scalability. Immense amounts of information can be stored in qubits. Unfortunately, it would not necessarily be useful to have hundreds of qubits in their own states of superposition. Instead, in order to take advantage of the scalability that quantum affords, qubits need to be entangled.

Qubit entanglement is the connected states of one or more qubits. In a system where two qubits are entangled, qubit one is measured as the opposite of qubit two. The key to creating useful and productive quantum algorithms is the underlying state of mass entanglement. By creating complex entanglements, you are then able create a web of superpositions. A classical computer is able to model superposition to a decent extent; however, entanglement is the key differentiator to classical computing. A classical computer cannot model a state where two bits have no value but opposite values. A quantum computer can. While entanglement is perhaps the most important part to quantum information it is also an achilles heel. Entangled states are extremely fragile and can easily be ruined by interference. As a result, quantum computers must be delicately constructed with many exhaustive features. In order to keep stable states, quantum computers must have a controlled environment that is extremely cold at -460 degrees Fahrenheit and completely still; otherwise, **decoherence** is risked. Decoherence is when

the quantum state breaks down and measurement errors occur. It can come about due to any number of factors including stray air particles or photons. The important part about decoherence is not the physics behind it but the high probability that it might occur.

Qubits are operated on through quantum gates. Both classical and quantum computers use what are called logic gates. These are simply booleans: yes or no operations. The only difference is that classical computation deals in classical bits and quantum computation in qubits. Because of this, however, quantum gates can utilize superposition and entanglement which makes the logic of quantum computers far more complex. This complexity is best described using matrices. A state is often transcribed using a vector. For example, an electron with the state spin down, would be written as **|1>**. Or in column vector form:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Matrices are then used to transform states through a mathematical concept called matrix multiplication. Below is an example of a state being transformed from spin up to spin down.

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Don't be alarmed if this looks daunting. This concept will be addressed in more detail. The main takeaway is that quantum gates work similarly to classical gates in that they take an input and give an output. They are however, extremely complex, especially as you add qubits. The above state change is a one qubit transformation. Matrix elements increase at a scale of 2^n x 2^n so the math behind these gates gets extremely dense. However, while there are plenty of gates that are quite intricate, many are simple and can be used to make elegant quantum algorithms.

Common Quantum Gates

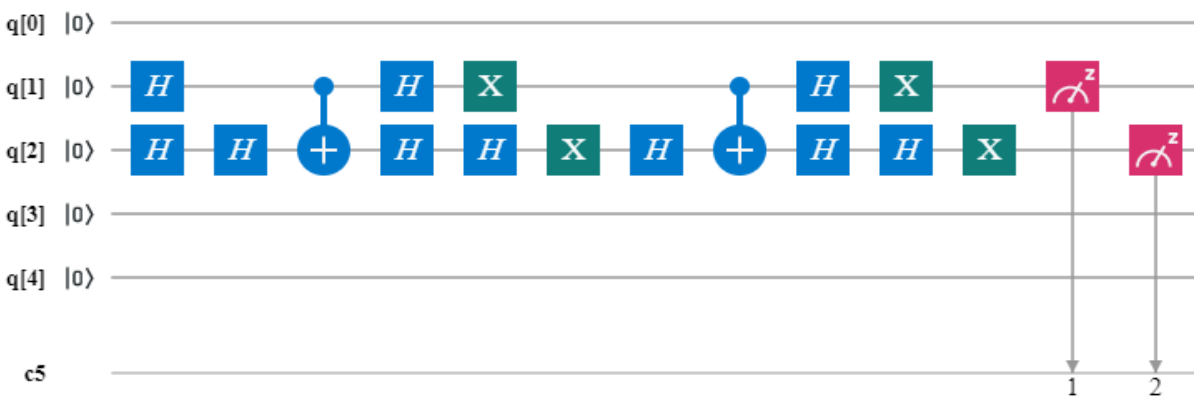
There are many different types of gates but the following are the most common. The Pauli X-gate is similar to the classical NOT gate. The denotation for the Pauli X-gate is a capital X. It changes the spin of the electron from down to up or up to down, subsequently changing the value of the qubit from 1 to 0 or vice versa. In this way, the X-gate is very similar to a classical gate in that it does not necessarily deal with superposition or entanglement but instead acts with binary output. The Hadamard gate, denoted as the H gate, is a much more "quantum" gate. It is a powerful gate that transforms a qubit into a superposition state. At first, qubits are initialized into a pre-set state. The Hadamard gate returns the qubits back to a more fluid level. Once a qubit passes through a Hadamard gate it becomes equally spin down and spin up and therefore more fully accesses the power of quantum computing. There are plenty more quantum gates, but these two are both the most simple and furthermore good representatives of the types of gates and will be used in the algorithms explained later.

Section 2: Popular Quantum Algorithms

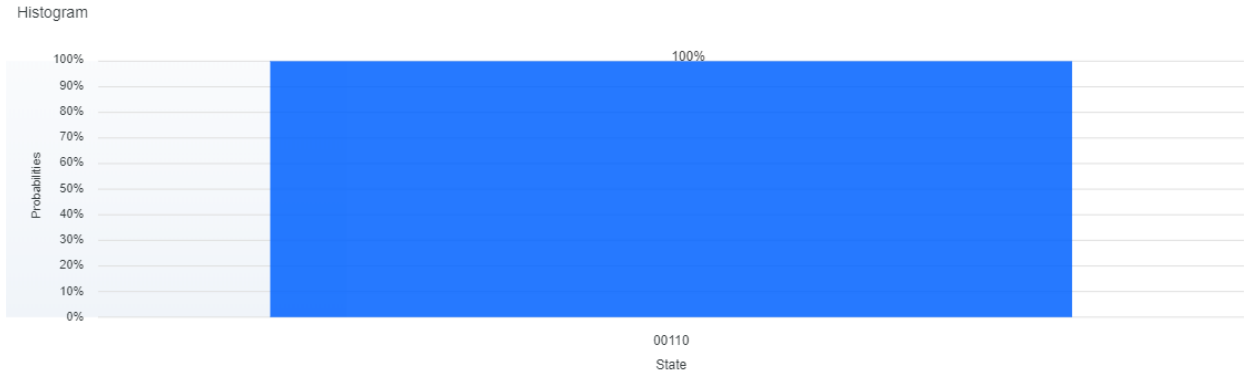
This paper predicts two core applications for quantum computation in political science research. First, it could be used as a research method and tool. The most likely and most studied application would be the use of quantum search algorithms. Especially as data increases at exponential rates, quantum computation could be used as a way to search complex, unstructured databases in unparalleled time. Second, quantum supremacy will undoubtedly result in diplomatic tension and discourse as well as require swift policy maneuvers. In this second use, possible areas of study include assessing quantum as a technology shock that could destabilize global information security and as an interesting policy challenge or through a security studies lens. The following will use two of the most famous quantum algorithms, Grover's Search Algorithm and Shor's Algorithm, to show the potential for quantum computation in these two respects.

Grover's Search Algorithm was invented by Lov Grover in 1996. It solves the problem of the unstructured search. An unstructured search problem attempts to find an element in a set of unordered elements. A classical solution would solve the problem linearly by looking at each individual element until eventually finding a match. One could think of this as putting a bunch of marbles in an enclosed box and trying to find one in particular. This would be done one by one until the correct marble was found. Quantum computers would take a different approach, leading to a quadratic speed up. This is slower than other quantum algorithms as they usually afford exponential time increases but is still significantly better than the classical solution. To better see the possibilities let's use a common card game as an example.

The following is the results of a version of Grover's search algorithm applied to a game of 4 Card Monte. 4 Card Monte is a game in which you lay 4 cards face down and hide a queen in one of the 4 cards. You then try to pick that hidden Queen in as few tries as possible. With a classical computer or via human effort, finding the queen would take 2.25 tries on average. The operation for this would be a linear search. Picking up one card at a time and running it through a boolean. Is it a queen? The output is either Yes or No. The quantum computer is able to find the hidden queen on the first try every time. This is due to the superposition state. By first time, this just means that there is only one output. The quantum computer can check all states at once.



IBMQ Case 1: Card set at position 11 in the Oracle



IBMq Code:

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[5];
creg c[5];
h q[1];
h q[2];
h q[2];
cx q[1],q[2];
h q[1];
h q[2];
x q[1];
h q[2];
x q[1];
h q[2];
cx q[1],q[2];
h q[1];
h q[2];
x q[2];
measure q[2] -> c[2];
measure q[1] -> c[1];
```

` The algorithm works by first applying two Hadamard (H) quantum logic gates to put the qubits in superposition. The second function is an oracle function or “black box” function that hides the queen in the position of our choosing. In the example, the oracle hides the queen in position 11. The third step is the inversion function that “discovers” the hidden queen. Finally, there are two measurement gates that produce the value.

Shor's algorithm is probably the most well-known quantum algorithm amongst those who are only tangentially aware of quantum computing. This is because if a quantum computer is built with enough qubits then it will be able to break RSA encryption, one the most popular methods of encryption in the world. RSA encryption works due to a mathematical principle called prime factorization. Prime factorization is simply finding the prime factors of a number. RSA leverages the computational difficulty of factoring large numbers to create a system that is mathematically secure. It would take longer than the lifetime of the universe to break current RSA encryption techniques using classical methods. Shor's algorithm proposes a solution to prime factorization problems in polynomial time, an exponential speedup from classical computation (Shor 1994). Current research has expanded on Shor's original findings and advanced the capabilities of the algorithm. A December 2019 paper published jointly by Google, KTH Royal Institute of Technology, and the Swedish Armed Forces proved how to factor 2048-bit RSA integers in only 8 hours (Gidney and Ekera 2019). In 2014 using only 4 qubits, a quantum computer was able to factor 56153, the largest published finding to date*[1] (Dattani and Bryans 2014). The Gidney and Ekera study was theoretical and would require a 20 million bits quantum computer to execute. However, using four qubits Dattani and Bryans were able to factor a large number. This is the conundrum of the duality of quantum computing. We may need millions of qubits to have massive consequences (Kim 2014), but we can make significant strides with only a handful of qubits. This will be the problem that policy makers will have to grapple with.

[1] A company called Zapata claimed to factor 1,099,551,473,989 but have to publish this study

Algorithm Conclusions

The above adaptation of Grover's Search Algorithm is no scientific achievement and is by all means a basic quantum algorithm and implementation. IBM does a similar experiment in their sales pitch for their cloud quantum computer and many tutorials exist to create models either exactly like this or for other algorithms of similar complexity. It is this simplicity however, that makes the algorithm significant. An undergraduate with average computation skills and little knowledge of quantum mechanics was able to access a quantum computer through the cloud and execute an unstructured search proving a quantum advantage. Imagine the potential for political science methods researchers with large university and institutional backing and experience with complex computation.

Shor's algorithm shows the technical workings of an algorithm that could disrupt internet security. Shor's algorithm and the multitudes of Shor based algorithms have a proven capacity to break prime factorization. There are plenty of theoretical papers and experiments that have physically proven this in a limited capacity. However, to fully access the power of Shor's algorithm, there needs to be quantum computers with more than 4 qubits and in the audacious range of millions if not billions of qubits. So how then do policy makers and researchers best treat quantum computers? After reading the above pages, you are now in the top percentile of people in the world who understand how quantum computing works. Whether experts predict the arrival of universal quantum computers in 10, 20 or 50 years what policy limitations should there be if any? Should there be more attention paid to policy questions about quantum computing or less? I would hope that the past pages have clouded your answer to these questions. Quantum computing is a policy

conundrum because it has an incredibly high ceiling but also a low floor. Current quantum technologies cannot do anything dangerous enough to warrant significant policy applications, however, with one advancement or one discovery, it could be one of the most dangerous cyber weapons in the world. On the other hand, would restrictions hinder the ability for quantum computers to solve groundbreaking medical problems? Would the fear of weaponized quantum technology prevent it from being used for early stage cancer detection or drug discovery (Solenov et al. 2014)? What is the balance for quantum regulation and policy?

Section 3: Applications

The majority of current Political Science Research looks at quantum computing from a security studies angle. Another interesting offshoot is the theoretical concept of the quantum mind. However, mainstream political science researches have not approached the subject and many prestigious political science journals have no publishing related to quantum. This includes zero relevant articles in either the American Journal of Political Science or the Quarterly Journal of Political Science. Even more surprising is quantum computing's absence in the computational political science journal Political Analysis. While quantum computing and quantum technology may be in developmental stages, once quantum computing matures it will quickly become a disruptive method and technology and thus must be studied now.

China is seemingly garnering the most attention, outside of the United States, as a quantum threat and serves as a good case study for the depth of political science quantum research. Researchers currently leading the academic charge on this issue are Elsa Kania and John Costello who are producing consistent literature about the Chinese threat from universal quantum technology. They claim that China is attempting to challenge the United States' position as quantum computing hegemon (Kania and Costello 2018). This push is a part of China's Thirteenth Five-Year plan that is placing a significant investment, in the area of billions of dollars, towards funding quantum research in universities and military labs. China has also begun to refocus university talent and strategic resource visions towards pursuing quantum computation. This has already proved dividends for China who now is the world leader in quantum computing patents related to cyber security (Kania and

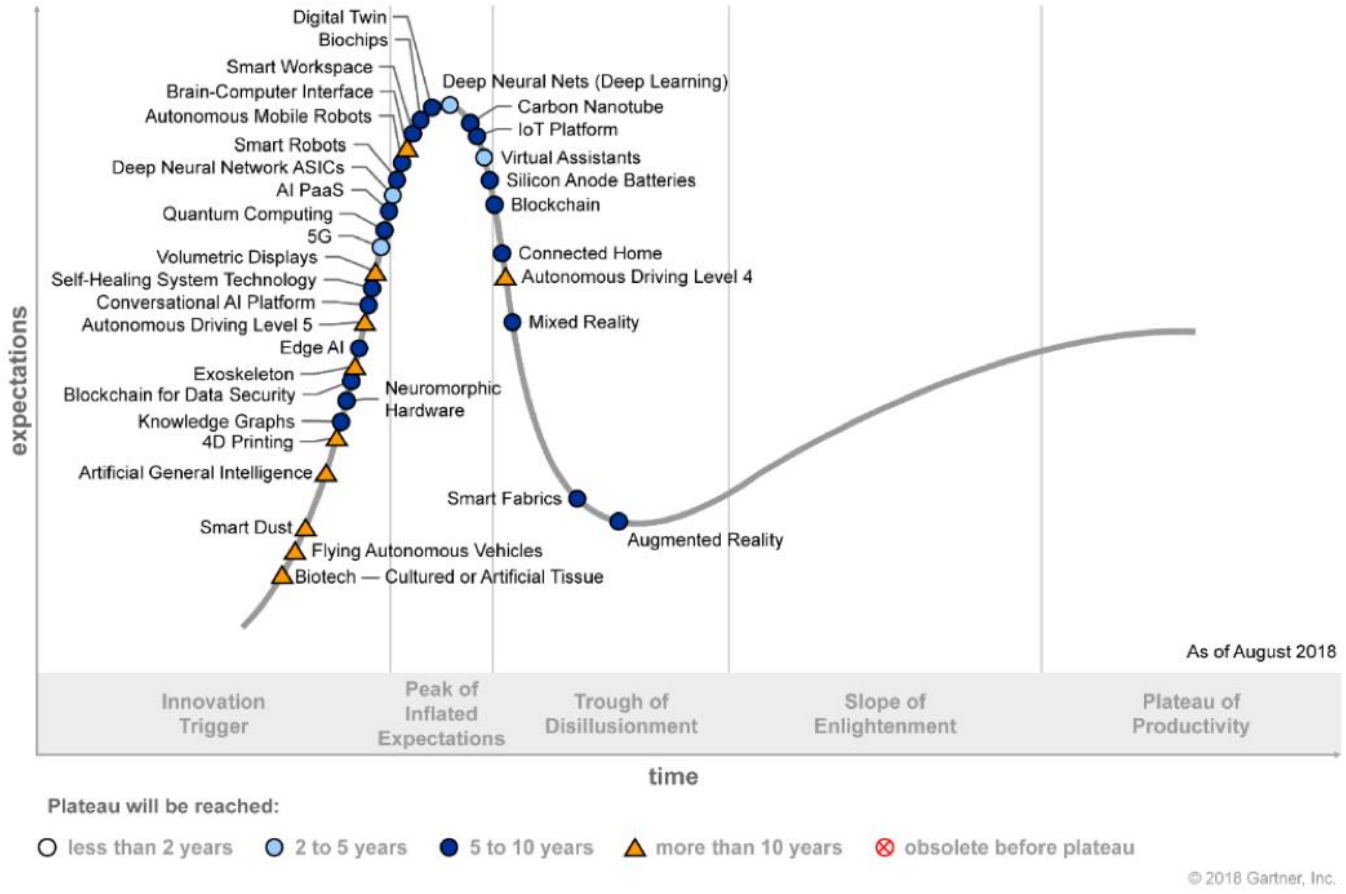
Costello 2018). This alone should garner more attention from policy makers and researchers alike. There has been plenty of research on the hegemonic challenge from China and cyber security is an area of notable contention. Furthermore, in their papers (Kania and Costello 2018) (Kania and Costello 2017), Kania and Costello contend that while quantum technology is still facing legitimate charges of utility, China is heavily investing in this potential and threatens the United States' economic and national security interests.

An abundance of literature and commentary can be found in private sector literature and industry publishing on the United States and Chinese quantum relationship. On one hand this makes sense, due to private sector leads, IBM and Google. However, it also questions further the absence of more political science literature. A CNN political analyst compares the United States-Chinese battle over quantum computing to the Space Race between the Soviet Union and the United States during the Cold War (Griffiths 2019). Another article examines the United States' National Quantum Initiative Act and its adequacy to help compete with China (Glass 2018). The point of the previous paragraphs is not to persuade towards any policy position or opinion of China but instead to note the glowing importance of more academic research on the topic. Quantum computing, in its universal state, poses a significant threat to US political and economic interests and if top scientists at Google and IBM are concerned about the future of quantum computing, so too should political scientists. Current developments should be further studied to determine the extent these concerns deserve merit.

In a separate political realm is Alexander Wendt's theory of the Quantum Mind. He argues that the brain is actually a quantum system or more specifically a quantum wave. Wendt further questions whether consciousness is also quantum, thus questioning the

legitimacy of all human analyses. If quantum computing is reverting computation back to the roots of computer science and rebuilding its principals, Wendt is reverting to the first ideas of consciousness and building from there. His book *Quantum Mind and Social Science: Unifying Physical and Social Ontology* is incredibly interesting, especially for the political philosopher and I would recommend it to any political scientist who seeks to challenge the status quo of the field; however, that is where this paper will leave this. The concept is worth mentioning but somewhat out of scope.

Quantum computing should be studied more in the social sciences despite its current state of development. The reality is that quantum computing is not a universal tool and fails to be of current widespread use. The goal for quantum computing is what is called **quantum supremacy.** This is the point at which a quantum computer can solve a problem that is practically impossible for a classical computer to solve. By practically impossible this means that a problem is either completely impossible or that it would take a long time to solve, as in thousands of years. Quantum computing is still years away from reaching quantum supremacy according to most estimates. The following figure is an estimate by Gartner from 2018 that shows the “hype cycle” of emerging technologies:



This analysis by Gartner is a good central estimate of the future for quantum computing. Quantum computing is most likely still in the peak of inflated expectations. According to Gartner, technologies in this cycle exhibit publicity with a number of success stories while experiencing many failures. They further state that while some companies may take action towards researching and using the technology, many will not. Nonetheless, while 5 to 10 years seems to be a good estimate, this also downplays the worldwide commitment to Quantum technologies. By 2018, three North American quantum technology companies, 1Qbit, D-wave Systems, and Rigetti had already acquired over 200 million dollars in investments alone (Gibney 2019). Countries around the world have also committed to public financing in quantum technology. In 2018, President Trump signed a

bill that invested 1.2 Billion dollars towards quantum technology. China has already eclipsed 2 billion dollars towards quantum investment and even countries such as India (1.12 Billion), Japan, Germany, and Canada have committed funds towards quantum computing research and development (Mehta 2020). Not to mention, major private companies such as Google, IBM and Intel are leading the charge with hundreds of millions of dollars in investments (Diederichs et al. 2018). The world is committing to quantum computing and so too should academics and Political Science academics in particular.

Despite the previously mentioned uses, there are other areas that political science researchers should look to implement quantum computation as a research method. Quantum computing has shown its greatest application in optimization problems and sampling problems. Quantum sampling is particularly popular due to Google's recent achievements in the area and it does have potential applications, however optimization problems will most likely be the best place for further exploration. This area is where scientists have had their greatest success and where quantum technology has developed its strengths. An optimization problem is one where a computer must find the best possible solution from all feasible solutions. Shor's algorithm and Grover's algorithm are both at their core matters of optimization. In this way, it may be most beneficial to classify quantum computing as an optimization tool. As a result, quantum machine learning would be the next logical area of potential research use. This area has been widely researched as a general computer science principal and should be further examined by political science methods researchers. A good starting place for this would be: (Schuld, Sinayskiy, & Petruccione 2014) and (Lloyd, Seth et al. 2013). While quantum computers may not be at the stage of maturity where they are universally useful today political scientists should

start to develop algorithms and use cases that will be of value when quantum computers reach supremacy.

Conclusion

Quantum computers are maturing and should be accessible to researchers in the next decade. Quantum computing seems to have a scary connotation in the media and to the general public that is aware of it. The advanced mathematics and difficult physics serve as a barrier to entry for many social science researchers. Hopefully the technical sections have dissuaded some of the fear or confusion. Especially as companies like IBM make their technologies more accessible to the public, the technical aspects will become less important for those hoping to utilize the technology in a mainstream way. They are however important for the researcher who attempts to use the technology in a new stream.

Quantum computing has not garnered the attention that it deserves by political science researchers. The technology will soon provide advanced speedups to solvable problems and even introduce new problems that were once deemed untouchable. On the other hand, most of the world's largest nations have invested in quantum technology and academia should take notice. Quantum computers will prove to be important in areas such as cyber security policy and security studies and will play an important role in global economic competition in the future. The aim of this paper was to educate and inspire political science researchers to grapple with the possibilities and consequences of quantum computing. By doing so, hopefully more attention will be paid to the topic.

Bibliography

Dattani, Nikesh S., and Nathaniel Bryans. “Quantum Factorization of 56153 with Only 4 Qubits.” 2014.

Desjardins, Jeff. “The 3 Types of Quantum Computers and Their Applications.” Visual Capitalist, 13 Mar. 2020, www.visualcapitalist.com/three-types-quantum-computers/.

Diederichs, Julian, et al. “VC Investment Analysis: Quantum Computing.” INSEAD, Apr. 2018.

Fürer, Martin. “Solving NP-Complete Problems with Quantum Search.” Lecture Notes in Computer Science LATIN 2008: Theoretical Informatics, pp. 784–792., doi:10.1007/978-3-540-78773-0_67.

“Gartner Identifies Five Emerging Technology Trends That Will Blur the Lines Between Human and Machine.” Gartner, www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine.

Gibney, Elizabeth. “Quantum Gold Rush: the Private Funding Pouring into Quantum Start-Ups.” Nature News, Nature Publishing Group, 2 Oct. 2019, www.nature.com/articles/d41586-019-02935-4.

Gidney, Craig & Ekerå, Martin. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.” (2019).

Glass, Paulina. “Congress's Quantum Science Bill May Not Keep the US Military Ahead of China.” Defense One, 17 Sept. 2018, www.defenseone.com/threats/2018/09/congresss-quantum-science-bill-may-not-keep-us-military-ahead-china/151319/.

Greenemeier, Larry. “How Close Are We-Really-to Building a Quantum Computer?” Scientific American, Scientific American, 30 May 2018, www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.

Griffiths, David Jeffrey, and Darrell F. Schroeter. Introduction to Quantum Mechanics. Cambridge University Press, 2019.

Griffiths, James. “US Just Moved Ahead of China in Quantum Computing. But the Race Isn't over Yet.” CNN, Cable News Network, 24 Oct. 2019, www.cnn.com/2019/10/24/tech/china-quantum-computing-intl-hnk/index.html.

“Hype Cycle Research Methodology.” Gartner, www.gartner.com/en/research/methodologies/gartner-hype-cycle.

Kania, Elsa B., and John K. Costello. “Quantum Technologies, U.S.-China Strategic Competition, and Future Dynamics of Cyber Stability.” 2017 International Conference on Cyber Conflict (CyCon U.S.), 2017, doi:10.1109/cyconus.2017.8167502.

Kania, Elsa B., and John K. Costello. China’s Quantum Ambitions. Center for a New American Security, 2018, pp. 6–13, QUANTUM HEGEMONY?: China’s Ambitions and

the Challenge to U.S. Innovation Leadership, www.jstor.org/stable/resrep20450.6. Accessed 6 Apr. 2020.

Kania, Elsa B. “China's Quantum Future.” Foreign Affairs, Foreign Affairs Magazine, 28 Sept. 2018, www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

Kim, Yoongu, et al. “Flipping Bits in Memory without Accessing Them: An Experimental Study of DRAM Disturbance Errors.” 2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA), 2014, doi:10.1109/isca.2014.6853210.

Koren., “A. The RSA Encryption Algorithm.” The RSA Encryption Algorithm Is One of the Most Widely Used Private Key Encryption Algorithms That Have Ever Been Invented, www.ecs.umass.edu/ece/koren/FaultTolerantSystems/simulator/RSA/new_page_5.htm.

Lloyd, Seth et al. “Quantum algorithms for supervised and unsupervised machine learning.” (2013).

Lund, A. P., et al. “Quantum Sampling Problems, BosonSampling and Quantum Supremacy.” Npj Quantum Information, vol. 3, no. 1, 2017, doi:10.1038/s41534-017-0018-2.

Mehta, Ivan. “India Finally Commits to Quantum Computing, Promises $1.12B Investment.” The Next Web, 3 Feb. 2020, thenextweb.com/in/2020/02/01/india-finally-commits-to-quantum-computing-promises-1-12b-investment/.

“New Insights. Tangible Outcomes. New Applied Now.” Accenture, www.accenture.com/us-en/success-biogen-quantum-computing-advance-drug-discovery arxiv.org/abs/quant-ph/9508027.

Morello, Andrea, director. Quantum Computing Concepts – Quantum Logic. UNSW, 2 May 2016.

Radu, Sintia.“Google Quantum Chief Fears China Will Soon Catch Up in Supercomputing.” U.S. News & World Report, U.S. News & World Report, www.usnews.com/news/best-countries/articles/2020-01-31/google-quantum-chief-warns-china-can-quickly-develop-supercomputers.

Roell, Jason. “Demystifying Quantum Gates - One Qubit At A Time.” Medium, Towards Data Science, 28 Feb. 2018, towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640.

Schuld, Maria, et al. “An Introduction to Quantum Machine Learning.” Contemporary Physics, vol. 56, no. 2, 2014, pp. 172–185., doi:10.1080/00107514.2014.964942.

Shor, Peter W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” SIAM Journal on Computing, vol. 26, no. 5, 1996, pp. 1484–1509., doi:10.1137/s0097539795293172.

Simon, D.r. “On the Power of Quantum Computation.” Proceedings 35th Annual Symposium on Foundations of Computer Science, doi:10.1109/sfcs.1994.365701.

Solenov, Dmitry et al. “The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine.” Missouri medicine vol. 115,5 (2018): 463-467.

Wendt, Alexander. Quantum Mind and Social Science Unifying Physical and Social Ontology. Cambridge University Press, 2015.

Wootters, W. K., and W. H. Zurek. “A Single Quantum Cannot Be Cloned.” Nature, vol. 299, no. 5886, 1982, pp. 802–803., doi:10.1038/299802a0.

Wright, John. “Lecture 4: Grover's Algorithm.” Lecture 4: Grover's Algorithm. 2015, https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf.